UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/516,236	03/01/2000	William A. Aiello	1999-0053	3274

7590 07/21/2004

Samuel H Dworetsky
AT&T Corp
P O Box 4110
Middletown, NJ 07748-4110

EXAMINER	
ZIA, MOSSADEQ	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/516,236	AIELLO ET AL.	
	Examiner	Art Unit	
	Mossadeq Zia	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 March 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15,18-20,22 and 34-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15,18-20,22 and 34-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date ~~5~~. No-mailed with #6 gm
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: On page 12 of the specification BTI is referenced as element 140 and so is the provisional server 140.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 7, 18 rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention.

4. Claim 7 recites the limitation "said tuple" in second line of the claim on page 3. There is insufficient antecedent basis for this limitation in the claim.

5. Claim 18, is dependent on cancelled claim 17. Accordingly, the claim will not been further treated on the merits.

6. Claim 34 recites the limitation "where a complement of key J"" on page 6. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Patent No. 5,153,919, Reeds, III et al.

9. Regarding claim 1, Reeds discloses a method of provisioning a user's broadband telephony interface comprising the steps of:

receiving the information authenticating a provisioning server (base station, mobile unit verifies string created by base station, Reeds, col. 8, line 63-68);

establishing a communication channel between the user and the provisioning server over which is transmitted authorization information from the user to the provisioning server (challenge, Reeds, col. 8, line 60-61); and

encrypting (hashing, Reeds, col. 3, line 15-16, col. 9, line 6-8) and transmitting a cryptographic key (SSD) associated with the user (mobile unit) to the provisioning server (authentication procedures, Reeds, col. 6, line 14).

10. Claims 8-20, 22, 34, 38 are rejected under **35 U.S.C. 102(e)** as being anticipated by Patent No. 6,094,485, Weinstein et al.

11. Regarding claim 12, Reeds discloses apparatus comprising:

a first interface to a landline user telephone (network connection, Weinstein, col. 1, line 49-50);

a second interface to a communication network (SSL session may include multiple secure connections) with access to a provisioning server (Weinstein, col. 8, line 62-63);

memory for storing cryptographic keys (server, Weinstein, col. 1, line 49-50, col. 8, line 2-4);

a processor connecting to the memory and the first and second interfaces for executing program instructions, the program instructions causing the processor to perform the steps of (client-server):

receiving a key of said provisioning server (certificate) and the information authenticating a provisioning server (server, Weinstein, col. 13, line 38-39);

generating a random key K (Weinstein, col. 8, line 1-4) and its complement (decryption is the reverse process, Weinstein, col. 10, line 46), a random session key SK and its complement, and a random audio channel key AK and its complement, where a complement of a key J is a key that decrypts messages message encrypted with said key J (symmetric cryptography, Weinstein, col. 4, line 65-67); and

sending to said provisioning server information that includes said complement of said K encrypted (secret) with said key of said provisioning server (public key from server's certificate), and a tuple encrypted with said K (encrypted pre-master secret message, Weinstein, col. 19, line 22-23), which tuple includes said complement of said SK, and said complement of said AK (Weinstein, col. 19, line 16-22).

12. Regarding claim 13, Weinstein disclose claim 12 above, and further show the processor also generates a public/private key pair (client sent a certificate), and sends the public key to said provisioning server (Weinstein, col. 13, line 53-55).

13. Regarding claim 14, Weinstein disclose claim 12 above, and further show the processor establishes a session communication channel with said provision server (Weinstein, col. 1, line 52-53).

14. Regarding claim 15, Weinstein disclose claim 14 above, and further show the processor communicates with said provisioning server over said session (Weinstein, col. 1, line 52-53).

15. Regarding claim 18, Weinstein shows claim (cancelled claim) 17 above, and further show a random nonce is included in said tuple (RSA pre-master secret message: random , Weinstein, col. 19, line 29).

16. Regarding claim 19, Weinstein shows claim 12 above, and further show the information authenticating the provisioning server is a digital certificate (Weinstein, col. 13, line 38-39).

17. Regarding claim 20, Weinstein shows claim 12 above, and further show the key K is a symmetric key (DES, Weinstein, col. 11, line 26-27).

18. Regarding claim 22, Weinstein disclose claim 12 above, and further show a hash (Weinstein, col. 11, line 6) is including with each transmission (MAC, Weinstein, col. 10, line 40-43).

19. Regarding claim 34, Weinstein shows a method of employing a user's broadband telephony interface (BTI) executed in said BTI in communication with a network, comprising the steps of:

sending a request to a provisioning server (client hello, Weinstein, col. 13, line 38);

receiving a key (certificate) of said provisioning server and information that authenticates said provisioning server (Weinstein, col. 13, line 38-39);

generating a random key (Weinstein, col. 8, line 1-4) K and its complement (decryption is the reverse process, Weinstein, col. 10, line 46), a random session key SK and its complement, and a random audio channel key AK and its complement, where a complement of key J is a key

that decrypts messages message encrypted with said key J (symmetric cryptography, Weinstein, col. 4, line 65-67);

sending to said provisioning server information that includes said complement of said K encrypted (secret) with said key of said provisioning server (public key from server's certificate), and a tuple encrypted with said K (pre-master secret message, Weinstein, col. 19, line 22-23), which tuple includes said complement of said SK, and said complement of said AK (Weinstein, col. 19, line 16-22); and

receiving an acknowledgement from said provisioning server (Finished message, Weinstein, col. 13, line 61-63).

20. Regarding claims 8, Weinstein shows claim 34 above, and further shows the information that authenticates the provisioning server is a digital certificate (server, Weinstein, col. 13, line 38-39).

21. Regarding claims 9, Weinstein shows claim 34 above, and further show any number of said keys taken from the set consisting of K, AK, and SK are symmetric keys, where a symmetric key is equal to its complement (key equality for encryption/decryption key is inherent to symmetric key encryption).

22. Regarding claim 10, Weinstein shows claim 34 above, and further show complement of said key K is a public key and said key K is a private key (Weinstein, col. 8, line 11-14).

23. Regarding claim 11, Weinstein shows claim 34 above, and further disclose a hash (Weinstein, col. 11, line 6) in included with each transmission (MAC, Weinstein, col. 10, line 40-43).

24. Regarding claim 38, Weinstein shows claim 34 above, and further show said step of sending to said provisioning server includes information encrypted with said key SK (symmetric cryptography, Weinstein, col. 4, line 65-67).

Claim Rejections - 35 USC § 103

25. The following is a quotation of **35 U.S.C. 103(a)** which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

26. Claims 2-7, 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 6,094,485, Weinstein et al. in view of Patent No. 6,675,216, Quatrano et al.

27. Regarding claims 2, Reeds discloses claim 34 above, but fail to show comprising the step of establishing a voice connection between said user and said network.

However, Quatrano teaches collaboration server 40 is preferably an enterprise-class, HTTP server application that enables agents 42 to visually interact with remote users over the Internet while the user and agent can also conduct a voice conversation about the visually shared material to participate in a collaborative session, a customer need only have an Internet-connected computer and a Java-enabled browser. The voice connection can take place over a single voice/data connection if the appropriate voice-over-IP (VoIP) hardware and software are in place (Quatrano, col. 4, line 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Weinstein as per teaching of Quatrano to to gain the benefit of collaborating

over the Internet (or an intranet) in which two or more participants, such as one or more users and an agent, can share dynamic content generated by a web site server (Quatrano, col. 1, line 52-55).

28. Regarding claims 3, Weinstein and Quatrano shows claim 2 above, and further show comprising said provision server sending a request to said user, over said voice connection with said complement of said key AK (Weinstein, col. 7, line 60, col. 8, line 62-63, col. 13, line 42-43).

29. Regarding claims 4, Weinstein and Quatrano shows claim 2 above, and further show the communication channel passes through said BTI (network connection, Weinstein, col. 1, line 50-51).

30. Regarding claims 5, Weinstein and Quatrano shows claim 4 above, and further show said key of said provisioning server is a public key (Weinstein, col. 13, line 38-39).

31. Regarding claims 6, Weinstein and Quatrano shows claim 5 above, and further show said acknowledgement is encrypted with said complement of said key SK (Finished message, Weinstein, col. 13, line 61-63).

32. Regarding claims 7, Weinstein and Quatrano shows claim 6 above, and further show a random nonce is included in said tuple (RSA pre-master secret message: random , Weinstein, col. 19, line 29).

33. Regarding claim 35, Weinstein and Quatrano shows claim 3 above, and further show the steps of:

relaying said request to said user (inherent in the network connection via gateways, router, switches etc);

receiving responsive information from said user (Weinstein, col. 13, line 53-55); and

forwarding said responsive information to said provisioning server, encrypted with said key AK (inherent in the network connection via gateways, router, switches etc.).

34. Claims 36-37 is rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 6,094,485, Weinstein et al. in view of Patent No. 6,675,216, Quatrano et al. in further view of Patent No. 6,681,327, Jardin.

35. Regarding claim 36, Weinstein and Quatrano show claim 35 above, but fail to show the steps of:

generating a public/private key pair; and

sending the generating public key to said provisioning server, encrypted with said key SK.

However Jardin teach key management protocol (ISAKMP/Oakley) which allows the destination device (provisioning server) to obtain (generate) a public key (Jardin, col. 2, line 26-28).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Weinstein and Quatrano as per teaching of Jardin to include IPSec to gain the benefit of secure exchange of packets at the IP layer.

36. Regarding claim 37, Weinstein and Quatrano and Jardin shows claim 36 above, and further show the step of receiving an acknowledgement message from said provisioning server, in response to said sending of generated public key, which acknowledgement message is encrypted with said complement of said key SK (Weinstein, col. 8, line 42-44).

37. Claim 39 is rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 6,094,485, Weinstein et al. in view of Patent No. 6,681,327, Jardin.

38. Regarding claim 39, Weinstein shows claim 38 above, but fail to show said information with said key SK provides an address of said BTI.

However, Jardin teaches IPSec security where Transport mode encrypts both the header (address) and the payload of a IP packet (col. 2, line 20-23).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Weinstein as per teaching of Jardin to include IPSec to gain the benefit of secure exchange of packets at the IP layer.

Allowable Subject Matter

39. Claims 36, 37 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

40. Applicant's arguments filed on page 8, dated 4-30-2004 has been fully considered but they are not persuasive.

Regarding claim 1, applicant contests that a provisioning server that there is not teaching for authenticating the base station. This examiner respectfully disagrees. See the newly formed rejection above. It can be said that the a mutual authentication takes place between the mobile unit and the base station (Reeds III, col. 8, line 50-68), where both units authenticate each other

by challenge/response steps. Futhermore, applicant contests on page 9 that a cryptographic key is cannot be asserted from the authentication string sited in Reed III. The independent merely states "cryptographic key associated with the user" which authentication string (Reeds III, col. 5, line 60-61, col. 6, line 7-10) shows. The authentication string is hashed/encrypted to produce SSD (shared secret data, Reeds III,col. 6, line 11-12) which is used to encryption of some signaling message (SSD-B, Reeds III, col. 6, line 14-18). Thusly the rejections stand.

Applicant's arguments with respect to claim 12-20, 22 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

41. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
7/9/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100